CLAIMS

1. A method for discovering a trust chain, at least comprising attribute delegations each with an issuer and a subject, that overall imparts a required attribute to a subject and is grounded in a known trusted issuer, the method involving the use of certificates as justification of associated attribute delegations and comprising the steps of:

a) - setting as a primary goal to be proved an attribute delegation from a known trusted issuer to said subject;

b) - seeking a backwards proof of said primary goal by a process of recursively taking a goal to be proved, starting with said primary goal, and decomposing it into subgoals one of which corresponds to an attribute delegation that is justified by an available certificate and has the same subject as the goal being decomposed, inability to decompose a subgoal that has not been proved causing the process to backtrack to a previous subgoal to seek a new decomposition of the latter;

c) - determining that a trust chain has been found upon the process of step (b) producing a chain of subgoals proved by corresponding certificates, that grounds in a subgoal justified by a justified attribute delegation that has as issuer the said known trusted issuer included in said primary goal.

2. A method according to claim 1, wherein the known trusted issuer included in said primary goal is a specifically identified entity that is inherently trusted by the discovery method at least in relation to said required attribute, said justified attribute delegation of step (c) being an attribute delegation that is justified by a corresponding certificate.

3. A method according to claim1, wherein the known trusted issuer included in said primary goal is the discovery method itself; said justified attribute delegation of step (c) being an attribute delegation that is justified either by an axiom inherently trusted by the discovery method, or by a corresponding certificate.

4. A method according to claim 3, wherein the discovery method, as said known trusted issuer, is represented in said primary goal and said axiom as a null issuer.

5. A method according to claim 1, wherein name mappings justified by corresponding certificates are permitted in a said trust chain in addition to attribute delegations, step (b) involving decomposing, as appropriate, a particular subgoal to be proved into a name mapping justified by an available certificate and a new subgoal corresponding to said particular subgoal but with the subject reverse mapped using said name mapping.

6. A method according to any one of the preceding claims, including as part of step (b):

-- maintaining a list of subgoals already generated and pursued,

-- checking each new subgoal against said list, and

-- terminating the process of step (b) in failure in the event of a new subgoal being found to already exist in the list.

7. A method according to any one of the preceding claims, wherein at least some of said certificates used in proving a said trust chain determined in step (c) as found have associated validity data, the method involving the further step of traversing the trust chain in a forwards direction from the trusted attribute delegation that grounds it and combining the validity data of all certificates involved to determine the validity of the overall attribute delegation represented by the chain.

8. A method according to claim 7, wherein step (c) involves storing the state of the process of step (b) prior to checking the validity of the trust chain found, this state being used to continue the process should the check of the validity of the initially found chain show that the chain is not valid.

9. A method according to any one of the preceding claims, wherein an attribute-delegation certificate used to prove a said subgoal has a subject-directed condition associated with it requiring that a specified subject must have a particular attribute in order for the delegation

to be valid, step (b) involving making this condition a further subgoal to be proved for the current chain being followed.

10. A method according to claim 1, wherein the process of step (b) is run to completion to find all trust chains, if any, proving the primary goal.

11. A method of selecting certificates to be sent to a resource which requires proof that a subject has a particular attribute before allowing use of the resource, this method involving carrying out the method of any one of claims 1 to 7 in respect of said subject and an issuer known, or likely, to be trusted by said resource; the certificates selected for sending to said resource being those associated with a trust chain, if any, thereby found.

12. A method of determining whether a resource requiring a user to have at least one predetermined attribute, is usable by a subject presenting certificates to the resource, this method involving carrying out the method of any one of claims 1 to 7 in respect of said subject and an issuer known and trusted by said resource and determining that use of the resource by the subject is permitted if a trust chain can be found.